

UNITED STATES DISTRICT COURT

for the
District of UtahFILED
2025 JAN 9 AM 9:56
CLERK
U.S. DISTRICT COURT

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

BLACK FUJIFILM FINEPIX S1000 DIGITAL CAMERA

Case No. 4:25-mj-00001 PK

SEALED

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ Utah _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2251	Production of Child Pornography
18 U.S.C. 2252A	Transportation/Receipt/Distribution/Possession of Child Pornography
18 U.S.C. 2423	Travel with Intent to Engage in Sexual Conduct with Minors

The application is based on these facts:
See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Lance Lange

Printed name and title

Sworn to before me and signed in my presence.

Date: January 9, 2025City and state: St. George, Utah

Judge's signature

United States Magistrate Judge Paul Kohler

Printed name and title

TRINA A. HIGGINS, United States Attorney (#7349)
 CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
 Attorneys for the United States of America
 20 North Main Street, Suite 208
 St. George, Utah 84770
 Telephone: (435) 634-4270
 christopher.burton4@usdoj.gov

**IN THE UNITED STATES DISTRICT COURT
 DISTRICT OF UTAH**

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR A BLACK FUJIFILM FINEPIX S1000 DIGITAL CAMERA	AFFIDAVIT Case No. 4:25-mj-00001 PK Magistrate Judge Paul Kohler
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR THREE OLYMPUS XD PICTURE CARDS, 2GB EACH	AFFIDAVIT Case No. 4:25-mj-00002 PK Magistrate Judge Paul Kohler
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR PANASONIC 750X VHS CAMCORDER, SERIAL D21A14242	AFFIDAVIT Case No. 4:25-mj-00003 PK Magistrate Judge Paul Kohler
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR TWO COMPACT VHS VIDEO CASSETTES	AFFIDAVIT Case No. 4:25-mj-00004 PK Magistrate Judge Paul Kohler

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR MOTOROLA PHONE MODEL XT2413V BEARING IMEI 352036364830180	AFFIDAVIT Case No. 4:25-mj-00005 PK Magistrate Judge Paul Kohler
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR TOSHIBA LAPTOP SERIAL NUMBER X8474730Q	AFFIDAVIT Case No. 4:25-mj-00006 PK Magistrate Judge Paul Kohler

AFFIDAVIT IN SUPPORT OF APPLICATION

I, Lance Lange (Affiant), a Special Agent with the Federal Bureau of Investigation, having been duly sworn, state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the items belonging to Brian Lee Reeve, further described in Attachments A-1 through A-6, for the evidence described in Attachment B.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, § 2510(7), and am empowered by law to conduct investigations of and to make arrests for federal criminal offenses. I have been so employed by the FBI since March 2018. I am currently assigned to the FBI Salt Lake City Division, St. George Resident Agency (RA), and assigned to investigate criminal violations, including enticement of minors, sexual exploitation of children, and other

crimes against children. As a special agent with the FBI, I have participated in and received training related to the investigation of crimes against children and crimes committed using the internet. I have conducted many search warrants and led multiple investigations related to the use of technical techniques in the commission of federal crimes.

3. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of cooperating witnesses, emails provided by witnesses, the review of documents and records related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that the Affiant or others have learned during the course of the investigation. The Affiant has set forth only the facts that are believed to be necessary to establish probable cause to believe that violations of 18 U.S.C. § 2251(a) (Production of Child Pornography); 18 U.S.C. § 2252A(a)(1) (Transportation of Child Pornography); 18 U.S.C. § 2252A(a)(2) (Receipt of Child Pornography); 18 U.S.C. § 2252A(a)(5) (Possession of Child Pornography); and 18 U.S.C. § 2423(b) (Travel with Intent to Engage in Sexual Conduct with Minors) have been committed.

4. There is also probable cause to search the items and/or information described in Attachments A-1 through A-6 for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that—has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252A, and 2423 (the “Target Offenses”) relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2251(a) prohibits an individual from employing, using, or persuading, inducing, or enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

b. 18 U.S.C. § 2252A(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

c. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually

explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce.

d. 18 U.S.C. § 2252A(a)(5) prohibits knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2423(b) and (e) prohibit, among other things, any person from travelling in interstate commerce for the purpose of engaging in illicit sexual conduct.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Computers and computer technology have transformed the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

8. The development of computers has changed this. Computers basically serve

four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can now transfer photographs from a digital camera directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images can also be stored online or in the "cloud."

11. The internet and its ubiquitous reach affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Service Providers such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found

on the user's computer in most cases.

13. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, *i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, *e.g.*, traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software (P2P) (which is described in more detail in the following paragraphs), when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

14. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser

disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

15. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may

have been used to create the data (whether stored on hard drives or on external media).

16. In addition, there is probable cause to believe that the computer and its storage devices, monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of the Target Offenses and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

17. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to

determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

INTRODUCTION REGARDING PREFERENTIAL SEXUAL OFFENDERS AND THE INTERNET

18. Based upon my experience and discussions with other law enforcement officers, your affiant has learned that there are many types of preferential sex offenders. Some of these offenders have a primary sexual interest in children and are often referred to as pedophiles. This affidavit deals with these types of offenders. Preferential sex offenders receive sexual gratification from actual contact with children and/or from fantasy involving children, through the use of photographs and/or digital images that can be stored on computer hard drives and other types of digital recordable media (floppy diskettes, writable compact discs, writable DVDs, etc.). Your affiant is aware that these types of sex offenders often collect sexually explicit material consisting of photographs, video tapes, books, slides, and digital images, which they use for their own sexual gratification and fantasy and to show children in an attempt to lower the child's inhibitions.

19. Your affiant has learned that the internet has provided preferential sex offenders with a virtually anonymous venue in which they can meet other people with the same or similar sexual interests. Preferential sex offenders also use the computer to electronically exchange pictures of children or of adults engaged in sexual activity with

children. These images are readily and easily available on the internet. These images can then be downloaded and stored on the computer or other forms of digital recordable media such as CDs, DVDs, USB thumb drives, floppy disks, etc., and then viewed on the computer monitor at any time. Preferential sex offenders will also participate in chat rooms in order to communicate with other like-minded individuals and to meet children. This communication serves to legitimize their conduct and beliefs. Your affiant also knows from training and experience that preferential sex offenders who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collections of child pornography. I also know that these individuals typically maintain their child pornography collections in the privacy and security of their homes, or other secure location.

MOBILE APPLICATIONS AND THE SEXUAL EXPLOITATION OF CHILDREN

20. Your affiant knows from training and experience that many involved in the sexual exploitation of children use mobile applications to facilitate the sexual exploitation of children. There are millions of applications or “apps” available for download to any user with access to the internet. Popular apps including Gmail, Instagram, Facebook, Facebook Messenger, Whatsapp, Snapchat and others are commonly downloaded to a mobile device or smart phone (Although apps can also be downloaded to other internet connected devices like a desktop computer or laptop computer.).

21. Many of these apps have a social media function which allows a user to create their own profile and communicate with other users. Depending on the application, the communication can occur as text messaging, voice messaging, and/or live stream video messaging. Apps also often allow for the sharing of files between users. These files can be images or videos and are often sent as attachments to a message. These files can then be stored online (for example in the message history or thread on an Internet Service Provider's servers) or downloaded to the individual's device(s).

22. Individuals with a sexual interest in children can and often do use social media applications to communicate with other individuals with a sexual interest in children. Your affiant has worked several cases where individuals with a sexual interest in children have used social media applications to obtain, distribute, and manufacture child pornography. Your affiant also knows that individuals with a sexual interest in children can, and often do use social media applications to communicate with minors for the purpose of obtaining sexually explicit images of the children with whom they are communicating. These individuals often use multiple applications to communicate with victims and often create a profile where they pretend to be someone else. Your affiant has been involved in several investigations where an individual with a sexual interest in children has used social media mobile applications to communicate with children for the purpose of obtaining sexually explicit images and videos of the child, or for the purpose of meeting the child in person to engage in illegal sexual conduct.

///

///

THE INVESTIGATION

23. On October 22, 2024, at approximately 10:46 am, Richfield City Police Department (RCPD) responded to a complaint at the Cedar Canyon Senior Apartments located at 175 E 600 N, #204, Richfield, UT. A meal delivery service representative (also known and referred to herein as complainant) arrived at the address of Brian Lee Reeve for a meeting regarding a meal delivery service. The complainant was invited in by Reeve, who was not prepared for guests and excused himself to change. While inside Reeve's apartment, the complainant noticed several sexually explicit photos hanging on the wall in the living room next to the TV. According to the complainant, the photos depicted a minor female she approximated to be 5-7 years old with blonde hair (hereinafter referred to as "Victim 1"). The complainant stated that the photos showed Victim 1 without clothing and with her legs spread open exposing her genitals. The complainant stated that when Reeve returned to the living room, he noticed the photos and quickly took them down out of sight. The complainant left and contacted the police.

24. RCPD officers responded to the apartment of Reeve shortly thereafter. RCPD questioned Reeve about the allegations, which he denied. Reeve then gave his consent for the officers to search his apartment. During that consensual search, officers located two photos of a minor male, approximately 5 years old, with brown hair (hereinafter "Victim 2"). The photos depicted Victim 2 without clothing and showing part of his genitals. When questioned about the photos of Victim 2, Reeve denied knowing who the boy was.

25. RCPD detectives submitted a search warrant for Reeve's residence, which was approved on the same day by the Sixth District Court Judge Goble. RCPD officers executed the search warrant.

26. During the search, a cardboard box was located in a bedroom/storage room. In the cardboard box, RCPD found three poster boards with pictures taped to them. The first poster contained five pictures, one of which depicted child sexual abuse material (CSAM). In that photo, Victim 1 is seen standing up without clothing, exposing her chest and genitals. The second poster had four pictures taped to it, all of which contained CSAM. For example, the bottom right photos showed Victim 1 laying on her back with her legs spread apart and an adult penis partially inserted in her genitals. The third poster contained four more pictures taped to the poster board, all of which depicted CSAM. The bottom right photo shows an adult male with his legs open and his penis out, wearing a plaid shirt and Victim 1 is holding his penis near her open mouth. The photos attached to the poster boards also depicted several items that appeared to match items in Reeve's apartment, including a floral blanket and a wooden foldable table.

27. In the same bedroom/storage room, RCPD located a black precision design camera bag with a black Fujifilm Finepix S1000 digital camera (Subject Device A-1). There was an Olympus XD 2GB storage card in the camera and two more Olympus XD 2GB storage cards in the bag (Subject Device A-2).

28. RCPD seized Reeve's cell phone, which was a blue-and-black Motorola cell phone model XT2413V, IMEI 352036364830180 (Subject Device A-5).

29. RCPD advised Reeve of his *Miranda* rights and Reeve agreed to speak with the RCPD detective. Reeve stated that the Fujifilm camera was his. Reeve consented and signed a consent form for RCPD detective to search the camera and cell phone. When the RCPD detective asked Reeve about the CSAM posters, Reeve admitted that he had put the poster boards in the cardboard box to hide them. When asked if he was the male depicted in the photos, Reeve initially admitted he was, but later changed his statement and said he was not the male in the photos. Reeve stated he did not know who the people or children were in the photos.

30. The RCPD detective powered on the Fujifilm digital camera to see if it worked, and immediately observed a photo that depicted an infant female child without clothing (hereinafter "Victim 3") and an adult penis. The RCPD detective powered down the camera at that time without viewing further.

31. In the front room area, RCPD found and seized a grey-and-black Panasonic 750x VHS camcorder, model PV-L453D, bearing serial number D21A14242 (Subject Device A-3) with a green bag. Inside the video recorder was a compact VHS tape and an additional compact VHS tape was found inside the green bag (Subject Device A-4).

32. Reeve was placed under arrest by RCPD and transported to the police department for additional interviewing. While in the interview room, Reeve was again advised of his *Miranda* rights. Reeve declined to speak with the detective at that time. Reeve was booked into Sevier County Jail on state charges of sexual exploitation of a minor.

33. On October 23, 2024, RCPD detectives submitted an affidavit for a State search warrant for the camera, camcorder, XD memory cards, and cell phone, which was later approved by the Sixth District Court Judge Goble.

34. While reviewing the contents of the Fujifilm camera and the XD memory cards, the RCPD detective observed 58 additional photos of CSAM depicting Victim 1 and Victim 3. Additional photos were seen of an adult female victim (hereinafter “Victim 4”) that appeared to depict Victim 4’s nude genital area while she was sleeping.

35. While reviewing the contents of the Panasonic camcorder, there was a video of Victim 3. In that video, Victim 2 is lying on pink, green, and white floral blanket with pink yarn strings throughout. An adult male suspect is also captured and he is wearing a blue, black, and white plaid long sleeve shirt. The child is crying in the beginning of the video and is only wearing a shirt which is pulled up around her neck. The child has no clothing on below her waist and her genitals are exposed. During the course of the video, the adult male suspect opens the child’s legs and begins to use his right hand to spread the child’s genitals apart. The suspect continues to touch the child’s genitals and starts to rub the inside of her genitals with his finger. As the suspect is doing this, it sounds like a phone is going off, possibly his own, so he stops and the video ends. It is obvious that the suspect’s right hand in the video appears to be that of an older male.

36. During the review of evidence, the detective noticed several items found or seen in Reeve’s apartment that were also seen in photos and the video. Specifically, photos and videos depicted the male suspect wearing a black, blue, and white plaid long sleeve shirt and detectives believed a similar shirt was seen in Reeve’s apartment during

the search. Some of the photos also showed a wooden foldable table that also appeared consistent with a table in Reeve's apartment. Finally, some of the photos depicted a unique pink and white floral blanket with pink yarn strings throughout and appeared to match a blanket in Reeve's apartment.

37. The RCPD detective reviewed evidence photos and bodyworn camera videos from the search of Reeve's residence and saw the same blue, black, and white plaid long sleeve shirt hanging up in the closet that was seen during the recorded sexual assault of Victims 1 and 3. The shirt was not seized during the initial search. The RCPD detective submitted an additional affidavit for a search warrant to go back into the apartment for the plaid shirt. During the search, RCPD detective located the blue, black, and white plaid shirt, size XXL hanging up in the closet and seized it for evidence.

38. During the investigation, RCPD discovered that Reeve may have had two U-Haul storage units assigned to him. RCPD detectives submitted an affidavit for a search warrant for the U-Haul storage units, which was approved on October 30, 2024, in the Sixth District Court by Judge Goble. After the search warrants were approved, RCPD discovered that U-Haul was misinformed and that only one storage unit was in the name of Reeve. As a result, RCPD executed only the search warrant on the storage unit that was in Reeve's name. In that storage unit, RCPD located a blue hard shell luggage bag. Inside, RCPD found seven photos of CSAM printed on HP Advanced photos paper. The photos were similar to those previously located on the XD memory cards located in Reeve's apartment. Additionally, a zip lock bag containing three pair of small underwear, which appear to be the size of a young female, were found in the luggage. Additionally in

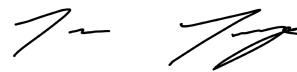
the storage unit, RCPD located an HP Officejet J4680 printer with a power cord and ink cartridge.

39. After Reeve's arrest, Victim 4 cleaned out Reeve's apartment. Victim 4 found a Toshiba laptop bearing serial number X8474730Q in the storage room of Reeve's apartment (Subject Device A-6). On October 28, 2024, Victim 4 provided the laptop and a written statement to RCPD.

40. On October 24, 2024, RCPD contacted the FBI for assistance with the ongoing investigation on Brian Reeve. From that date, the FBI has conducted numerous interviews and reviewed reports, evidence, and documents received from RCPD.

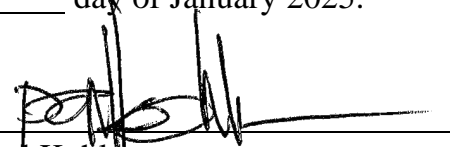
CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. Accordingly, by this Affidavit and Warrant, I seek authority for the government to search the property described in A-1 through A-6 for all of the items specified in Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents, records, and evidence identified in Attachment B.



Lance Lange
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN before me this 9th day of January 2025.



Paul Kohler
United States Magistrate Judge

Attachment A-1
(Physical Item to be seized and searched)

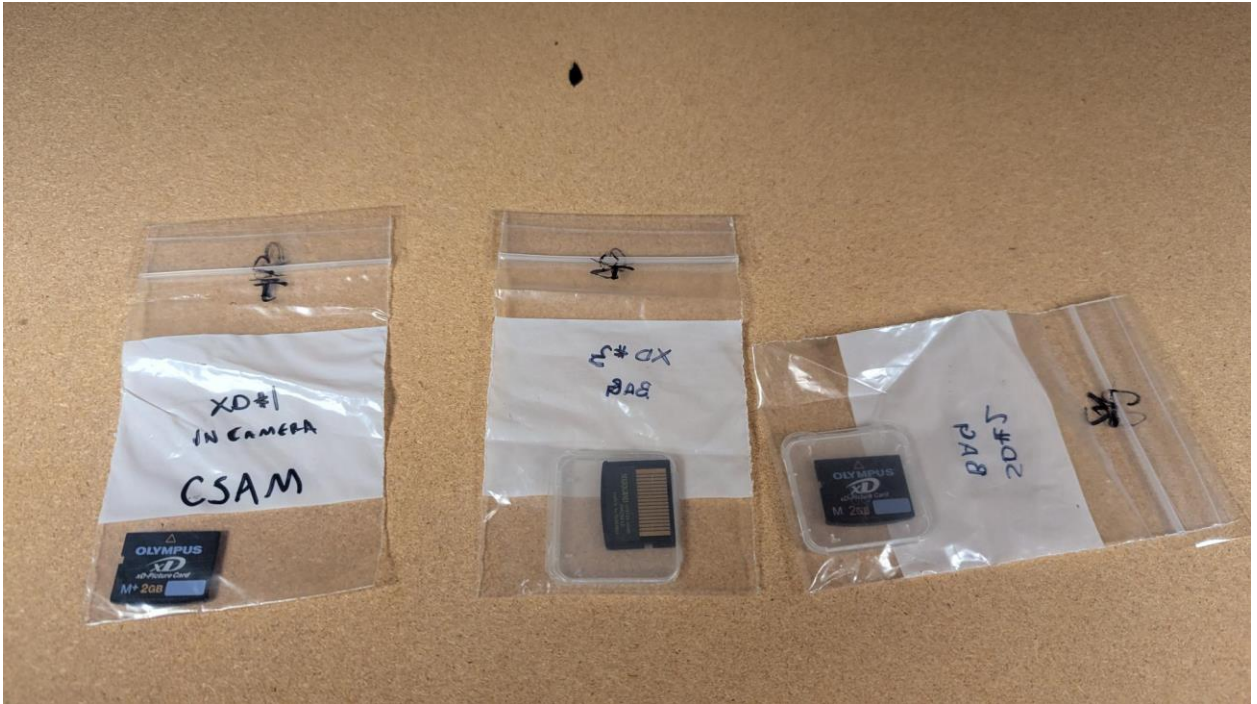
- Black Fujifilm Finepix S1000 Digital Camera (for purposes of attachment B).



Attachment A-2

(Physical Item to be seized and searched)

- Three Olympus XD Picture Cards, 2GB Each (for purposes of attachment B).



Attachment A-3
(Physical Item to be seized and searched)

- Panasonic 750x VHS Camcorder, Model PV-L453D Serial D21A14242 (for purposes of attachment B).



Attachment A-4
(Physical Item to be seized and searched)

- Two Compact VHS video cassettes (for purposes of attachment B).



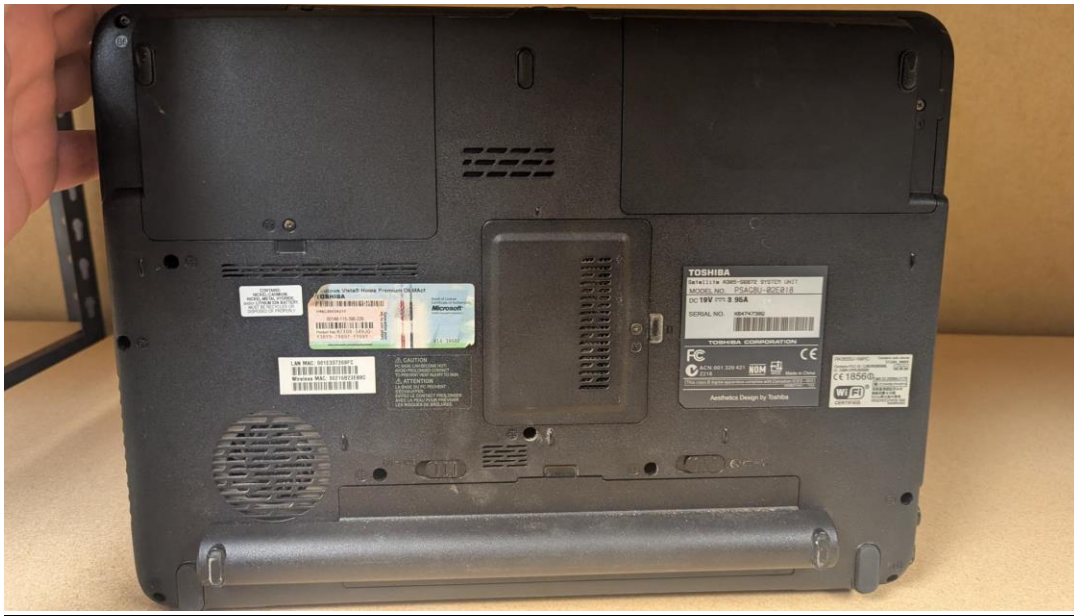
Attachment A-5
(Physical Item to be seized and searched)

- Motorola Phone Model XT2413V, IMEI 352036364830180 (for purposes of attachment B).



Attachment A-6
(Physical Item to be seized and searched)

- Toshiba Laptop Serial Number X8474730Q (for purposes of attachment B).



ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of application for a warrant to search Subject Devices A-1 through A-6, which are more specifically identified in the body of the application and in Attachment A (“Subject Devices”), that can be used to store information and/or connect to the Internet, or which may contain mobile devices, for records and materials that are fruits, evidence, or instrumentalities of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252A(a)(5), 18 U.S.C. § 2252A(a)(1), 18 U.S.C. § 2252A(a)(2), and 18 U.S.C. § 2423 (the “Target Offenses”). These records and materials are more specifically identified as:

1. Child pornography as defined in 18 U.S.C. § 2256(8);
2. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;
3. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items;
4. Any and all records and materials, in any format and media (including, but not limited to, text messages, SMS messages, picture/video messages, social media communication, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the Target Offenses;
5. Records and information evidencing occupancy or ownership of the Subject

Device described above, including, but not limited to, sales receipts, registration records, records of payment for Internet access, usernames, passwords, device names, and records of payment for access to newsgroups or other online subscription services;

6. Stored electronic data and related digital storage relating to Global Positioning System (“GPS”) data;

7. Records evidencing the use of the Subject Device’s capability to access the Internet, including: records of Internet Protocol addresses used and records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

8. Images and videos, to include any metadata identifying the date and location of the Subject Device at the time of the creation, receipt, transfer, or possession of a photo or video pertaining to the Target Offenses;

9. Evidence of who used, owned, or controlled the Subject Device at the time the things described in this warrant were possessed, accessed, received, created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

10. Evidence of software that would allow others to control the Subject Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and evidence of the lack of such malicious software;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Device;
12. Evidence of the times the Subject Device was used;
13. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Device.